Atty Docket No. ENI-037

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | | |
|---|---|---|---|
| Applicants: | Richard Bussiere et al. | | |
| Serial No.: | 10/713,560 | | |
| Filed: | November 14, 2003 | | |
| For: | DISTRIBUTED INTRUSION RESPONSE SYSTEM | | |
| Assignee: | Enterasys Networks, Inc. | | |
| Examiner: | Thomas M. Szymanski | | |
| Art Unit: | 2134 | Confirmation No. 8242 | Paper No. 13 |

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

**DECLARATION OF RICHARD GRAHAM PURSUANT TO 37 CFR § 1.131**

Dear Sir:

In support of my claim of prior invention of the invention described in the referenced application in view of the Sung et al. reference cited in the June 29, 2007, office action, I hereby declare as follow:

1. My name is Richard Graham. I am an applicant and co-inventor of the invention described and claimed in the referenced patent application.

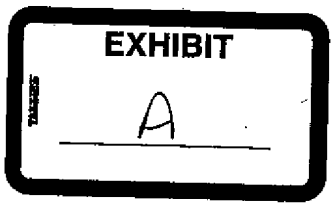
2. In association with others, I conceived of the invention described in the application before April 14, 2003. On January 2, 2003, I received from co-inventor Richard Bussiere a copy of an email communication sent to Chris Caseiro, the patent attorney processing the referenced application. A copy of the January 2, 2003, email message from Mr. Bussiere to Mr. Caseiro that I received is attached hereto as Exhibit A. The email communication that I received included a copy of a standard Enterasys Invention Disclosure Form and a supplemental invention description regarding the Distributed Intrusion Response System described in the referenced patent application. A copy of the standard Enterasys Invention Disclosure Form as I received it on January 2, 2003, is attached hereto as Exhibit B. A copy of the supplemental invention description as I received it on January 2, 2003, is attached hereto as Exhibit C.

2. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are

punishable by fine or imprisonment, or both, under 18 USC 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued.

By: _____
Richard Graham, Applicant

Date: Oct. 23, 2007




**From:** Bussiere, Dick
**Sent:** Thursday, January 02, 2003 3:31 PM
**To:** Caseiro, Chris
**Cc:** Graham, Richard
**Subject:** Patent Disclosure

Please find attached a patent disclosure and technical description for a distributed intrusion response system.

Thanks,

-d


Distributed ntrusion Response..


disclosure.doc (52 KB)

EXHIBIT

B

Invention Title _____
File No. _____
Date _____

ENTERASYS NETWORKS™

# INVENTION DISCLOSURE FORM

The purpose of this form is to assist inventor(s) in the preparation of an invention disclosure. The object is to minimize the amount of time that the inventor(s) must spend in processing a patent application without minimizing the importance and scope of the invention. The questions are designed to elicit enough information about the invention (e.g., the perceived novel features, what problem(s) it solves, why it is better or different from known existing technology, etc.) to assist the Intellectual Property Review Council (IPRC) make an informed decision about protection of the described invention.

If you have any questions regarding this form or the patent application process, please contact the Patent Counsel, Chris A. Caseiro, at (603) 337-1754 or ccaseiro@enterasys.com.

The following information is submitted to the IPRC as the basis for a preliminary patentability investigation and, should the IPRC approve the disclosure for protection, it will be used by our outside patent lawyers in preparation of a patent application for filing in the United States Patent Office and, in some instances, in other countries:

1. Title of Invention: Distribited Intrusion Response System

2. Provide a summary of the invention: Respond to network intrusion without prior knowledge of policy enforcement device on edge, learn location of attacker and block attack as close as possible to source.

3. Describe what you believe to be the point of novelty of the invention: The proposed approach is novel in that no prior knowledge of the actual network element which will be used to block the attack is required. This means that the number of security policy enforcement points is potentially infinite; any network element can be thought of as a device which is capable of enforcing security policy. This in effect distributes the intrusion response mechanism.

4. Describe the problem(s) solved by the invention: The problem of responding to an intrusion when there is no centralized network "choke point" where this can be accomplished; enables previously unused security policy enforcement points to be leveraged even when the intrusion detection function has no prior knowledge of the existence or locations of these devices.

5. To the best of your present knowledge, describe the current state of the art and how your invention is different. This does not require you to conduct an independent review or search of the field of your invention. Instead, please rely on your present knowledge: The current state of the art is to use a single "choke point" within the infrastructure, rather than a distributed approach.

6. Attach to this Disclosure any relevant notes, sketches, drawings, schematics, photographs, test results, test reports, presentations that describe the invention: Attached.

7. Identify whether the invention has been:
   (a) Incorporated in any tests or experiments? Yes or No
   If Yes, approximate date of first incorporation: No
   (b) Offered for sale? Yes or No
   If Yes, date of first offer for sale: No
   (c) Sold? Yes or No
   If Yes, date of first sale: No
   (d) Described in printed publication?
   If Yes, date and name of publication: None
   (e) Used other than at an Enterasys facility? Yes or No
   If Yes, where first used externally: No
   If used externally, date and purpose of such first external use:
   (f) Was the invention developed in whole or in part under a government contract? Yes or No
   If Yes, provide contract number(s): No

8. Is this invention embodied in a product presently being made? Yes or No
   If Yes, date of first fabrication: No

9. Will a product embodying this invention be made, sold, or offered for sale in the future? Yes or No
   If Yes, approximate dates of planned first fabrication, first offer for sale, and first sale: No

10. Was the invention conceived of or developed as part of a joint project with another person or persons not employed by Enterasys? Yes or No
    If Yes, identify each such person(s) and the name(s) of such person(s)' employer(s): Mark Townsend, Steve Pettit, John Roese

11. Was the invention disclosed to anyone else not employed by Enterasys? Yes or No
    If Yes, identify party to whom the invention was disclosed: No
    If Yes, was the disclosure made under a Non-Disclosure Agreement (NDA)? Yes or No
    If No NDA, identify the date(s) and location(s) of the disclosure:

12. Please identify any prior public documents or products of which you are aware that may be relevant to the novelty of your invention. (Please note that you are not required to seek such information, simply describe the information of which you are aware.): None

13. Date you first thought of the invention: June 2001

14. Do you have any documentation establishing when you first thought of the invention? Yes or No
    If Yes, attach such documentation to this disclosure.

First Named Inventor:
Full Name of Inventor: Richard Bussiere
Citizenship: USA
Residence Address:

Post Office Address (if different from above):
Telephone extension and Building:
Manager's name:

_____ _____
(Signature) (Date)

Second Named Inventor:
Full Name of Inventor: Mark Townsend
Citizenship:
Residence Address:
Post Office Address (if different from above):
Telephone extension and Building:
Manager's name:

_____ _____
(Signature) (Date)

Third Named Inventor:
Full Name of Inventor: Steve Pettit
Citizenship:
Residence Address:
Post Office Address (if different from above):
Telephone extension and Building:
Manager's name:

_____ _____
(Signature) (Date)

Third Named Inventor:
Full Name of Inventor: John Roese
Citizenship:
Residence Address:
Post Office Address (if different from above):
Telephone extension and Building:
Manager's name:

_____ _____
(Signature) (Date)

**FOR INVENTOR'S MANAGER**

Invention Title _____
File No. _____
Date _____

Disclosure Read and Approved ___ Disapproved ____ for Submission to IPRC:

Manager's Name:
Telephone extension and Building:

_____ _____
(Signature) (Date)

**FOR RESPONSIBLE IPRC MEMBER**

Disclosure Read and Approved ____ Disapproved ____ for Submission to IPRC:

Responsible Member's Name:
Telephone extension and Building:

_____ _____
(Signature) (Date)

EXHIBIT

C

# Distributed Intrusion Response System

The Distributed Intrusion Response System (DIRS) is a plurality of components which is intended to cause a dynamic response to a detected intrusion. The purpose of the DIRS is to:

- Stop a detected attack in a **fine-grained fashion** by leveraging policy enforcement controls available at the edge of the IT infrastructure
- Prevent detected attacks from spreading, through an early reaction mechanism
- Only disable protocols (i.e. L4) , physical addresses (i.e. L2) or logical addresses (i.e. L3) which are active participants in the attack, or protocols which are likely to be used in a further attack, while leaving other protocols enabled
- Dynamically disable protocols which are abused, leaving other productive protocols enabled
- Minimize effects of IDS false positives

**The DIRS does this by:**

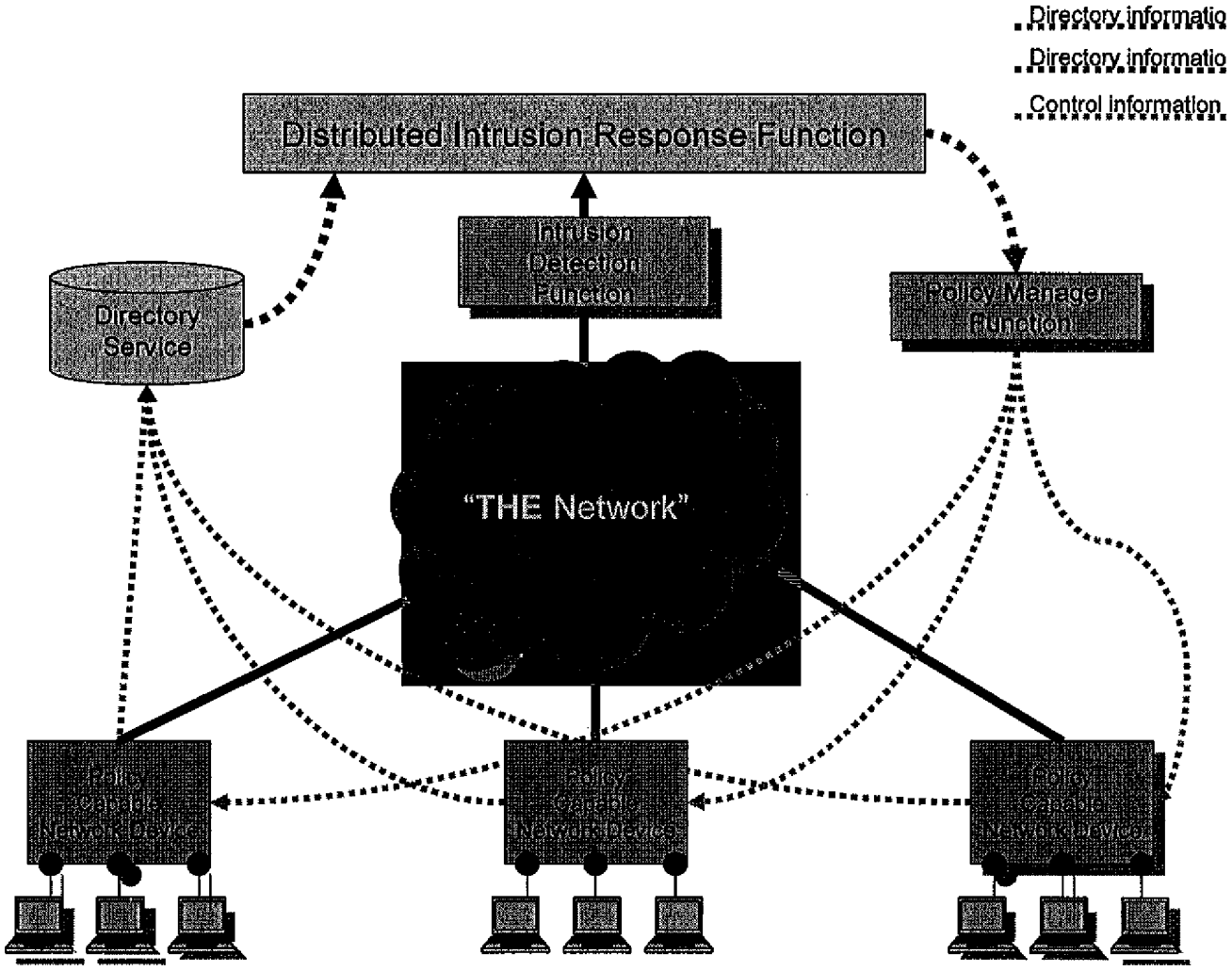
- Detecting a probable attack through 'traditional' IDS methods, either host based or network based
- Identifying the source of the attack
- Determining where in the network topology the attack was originating from, for example the physical (or logical) switch port
- Verifying the legitimacy of the attack origin (prevent IP address spoofing attacks from causing denial of service to legitimate end users)
- If available, determine WHO is generating the attack
- Block the attack at the point of entry; either the specific protocol or protocols, the source MAC address, and/or the source IP address
- Generate an alert to the system administrator

**The components of the DIRS are:**

- A centralized or distributed Intrusion Detection Function or systems; which monitor the network or networks for malicious or potentially malicious activities
- Policy Capable Network Devices, which are capable of enforcing L2, L3, and L4 policies in any combination
- The same network security policy devices (discussed above) having the ability to generate L2 location information, L2-L3 mapping information, and having the ability to forward this information to a directory service (a distributed directory)
- A Directory Service to provide the location of a physical device within the network topology.
- A Policy Manager Function which is responsible for configuring and controlling network security and utilization policies

- The Distributed Intrusion Response Function itself, which is responsible receiving information from the Intrusion Detection System and the Directory service, and then coordinating a response with the Policy Manager function

These components are shown in the illustration below:




**Operational Model briefly described:**

- Policy Capable Network Device "learns"
  - Attached device L2 physical (MAC) address
  - Attached device L3 logical to physical (i.e. MAC to IP) address binding
- Policy Capable Network Device reports learned topology information to directory service; included in this information is information relating to specific identification of Policy Enforcement Function (i.e. IP address of switch or router)
- Intrusion Detection Device monitors network for malicious activities

- On detection of malicious activity, if Intrusion Detection Function policy for the activity indicates that Intrusion Response is required, Intrusion Detection Function contacts Directory Service with source IP address of captured packet
- Directory Service replies with L2 (MAC address) and information sufficient to identify Policy Enforcement Device such as a switch, router or firewall to which the attacker, as identified by L3 IP address, is attached
- Distributed Intrusion Response Function will determine if IP address is legitimate by testing for presence of it using a technique such as 'ping'
- Distributed Intrusion Response Function requests that Policy Manager Function modify security policy being applied– Policy Manager applies policy; this is an important step since the policies must remain consistent. Having changes to policies without the knowledge of the Policy Manager would result in inconsistencies.
- Policy Manager modifies policy in Policy Capable Network Device, by sending control information to the device (i.e. SNMPv3) such that some or all of the following are accomplished:
    - Further network access by the device is blocked completely (i.e. MAC address filter is installed
    - Access by the IP address (only) is blocked (L3 filter installed)
    - Access or use of the offending protocol is blocked (L2/L4 or L3/L4 protocol is blocked
    - Limit bandwidth from, to, or from and to the device
    - Direct traffic to a honeypot or other monitoring device
    - Direct traffic to a simulation device, such as a simulated network

**Novel Concepts:**

The concept of an intrusion detection system generating an active response to a detected event is not new. For example, Dragon does this with the "shun" and "snipe" features. Unfortunately, the current implementation is static in nature in that it cannot take into account network topology. The device which will perform the shunning, for example, must be known in advance and "hard coded".

The proposed approach is novel in that no prior knowledge of the actual network element which will be used to block the suspected traffic is required. This means that the number of policy enforcement points is infinite; any network element can be thought of as a device which is capable of enforcing security policy. This in effect "distributes" the intrusion response mechanism – creating in effect a "web". On detection of an attack, the network element which services the attacking device is learned from the directory service. The network is then reconfigured to modify the authorization for the offending client machine.

**Possibly patentable ideas include:**

- Apparatus for accumulating topology information in an intrusion detection system

- Apparatus for determining connection point of end station within an intrusion detection system
- Mechanism for automating intrusion response mechanism

**Implementation Ideas:**

The current concept is to leverage the existing NetSight "Compass" application as the directory service. Compass accumulates the information from Enterasys switches. Compass would be bundled with Dragon as an option which would enable this functionality. Some development work would need to be done to give Compass an API which Dragon could leverage and use to query the directory.

Dragon should have a flexible API which would allow it to "plug-in" to applications other than Compass which are capable of collecting directory and network topology information.

It may also be quite interesting to develop a Compass plug-in which would allow it to be extended to support third-party switches which are capable of collecting L2, L3 and L4 information and enforcing L2, L3 and L4 policies.